(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 juillet 2003 (24.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/061193 A1

(51) Classification internationale des brevets⁷ : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR02/04335

(22) Date de dépôt international :
13 décembre 2002 (13.12.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/00107 4 janvier 2002 (04.01.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 14, rue Emile Dron, F-61100 Flers (FR).

(74) Mandataire : **JEUNE, Pascale**; France Telecom R & D/VAT/PI, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD AND DEVICE FOR ANONYMOUS SIGNATURE WITH A SHARED PRIVATE KEY

(54) **Titre :** PROCEDE ET DISPOSITIF DE SIGNATURE ANONYME AU MOYEN D'UNE CLE PRIVEE PARTAGEE

(57) **Abstract:** The invention concerns a method and a system for anonymous cryptographic signature of a message. The method consists in completing the anonymous signature which is calculated (13) with a private key common to the set of members of a group authorized to sign and unknown to all revoked members. Said private key is updated (8, 11) at group level upon each revocation within the group and at member level only upon anonymous signature of a message by said member. The system consists of as many cards as there are members in a group and a device comprising a first calculating means.

(57) **Abrégé :** La présente invention se rapporte à un procédé et à un système cryptographique de signature anonyme d'un message. Le procédé consiste à compléter la signature anonyme avec une signature additionnelle qui est calculée (13) à l'aide d'une clé privée commune à l'ensemble des membres d'un groupe autorisés à signer et inconnue de tous les membres révoqués. Cette clé privée est mise (8, 11) à jour au niveau du groupe à chaque révocation au sein du groupe et au niveau d'un membre uniquement lors d'une signature anonyme d'un message par ce membre. Le système se compose d'autant de cartes à puce que de membres dans un groupe et d'un dispositif comprenant un premier moyen de calcul.

WO 03/061193 A1

PROCEDE ET DISPOSITIF DE SIGNATURE ANONYME AU MOYEN D'UNE CLE PRIVEE PARTAGEE

Domaine de l'invention

La présente invention se rapporte au domaine des télécommunications et plus particulièrement à la sécurisation des transmissions, en particulier pour des services, qui fait appel à la cryptographie.

Etat de l'art

Pour authentifier l'origine d'un document transmis par des moyens de télécommunication, il a été développé des mécanismes de signature électronique. Il faut noter que les termes transmission sous forme électronique sont couramment utilisés pour qualifier une transmission d'un document par des moyens de télécommunication. Les documents dont il est question dans le contexte de l'invention se présentent obligatoirement sous forme numérique par opposition à une présentation sous forme papier ; le terme message est utilisé dans la suite de la demande pour désigner ce type de document. Les mécanismes de signature électronique les plus courants reposent sur des techniques de cryptographie dites à clé publique qui mettent en jeu une entité dite autorité de confiance. Habituellement, cette autorité de confiance génère des certificats pour le compte d'utilisateurs des procédés courants à clé publique ; ces certificats établissent un lien entre une clé publique et l'identité du propriétaire de cette clé. Pour mettre en œuvre un tel procédé, l'individu signataire du message doit préalablement se faire certifier auprès de l'autorité de confiance en lui communiquant au moins sa clé publique et son identité. Lors de sa mise en œuvre, le procédé de signature calcule une signature électronique du message en prenant en compte d'une part le contenu du message et d'autre part la clé privée de l'individu. Le signataire transmet au destinataire le message, la signature et son certificat. Le destinataire du message vérifie la signature électronique du message à l'aide d'au moins la clé publique et du contenu du message.

Pour des applications particulières, telles que le vote électronique, les enchères électroniques ou le paiement électronique anonyme, il est nécessaire de pouvoir disposer d'une signature électronique dite anonyme. Une signature électronique anonyme a les mêmes caractéristiques qu'une signature électronique sauf que le destinataire ne peut déterminer l'identité du signataire ; le signataire garde l'anonymat. Toutefois, le destinataire peut s'adresser à l'autorité de confiance qui dispose, par l'intermédiaire du certificat, d'un moyen pour lever l'anonymat.

Art antérieur

Parmi les différents types de signature anonyme, il existe un type particulier appelé signature anonyme de groupe. Un procédé de signature anonyme de groupe permet à chaque membre d'un groupe de produire une signature électronique qui soit caractéristique du groupe. Le destinataire d'un message accompagné d'une signature anonyme de groupe peut vérifier que la signature a été produite par un des membres du groupe. Toutefois il ne peut déterminer, parmi les différents membres du groupe, le membre dont il s'agit.

Dans le contexte de l'invention, un groupe est un ensemble d'individus qui se déclarent auprès d'une autorité comme appartenant à un même groupe. Lors de cette déclaration, chaque individu interagit avec l'autorité de confiance selon un protocole déterminé à l'issue duquel l'individu obtient une clé privée, associée à une clé publique de groupe préalablement déterminée par l'autorité de confiance, et l'autorité et l'individu obtiennent un identifiant de l'individu associé à cette clé privée. Chacun de ces individus est dans la suite de la demande désigné par le terme de membre. Un exemple d'un tel protocole est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. La même interaction intervient lors de l'arrivée d'un nouveau membre. L'existence d'un groupe se traduit du côté de l'autorité de confiance par l'attribution au groupe d'une clé publique dite de groupe et par l'attribution à chaque membre d'une clé privée associée à la clé publique, différente pour chaque membre, et d'un identifiant. A l'aide de sa clé privée, un membre peut produire une signature anonyme de groupe d'un message de son choix. Un destinataire quelconque peut vérifier que cette signature a bien été produite par un des membres du groupe à condition d'utiliser la clé publique de groupe. A l'issue de la vérification, le destinataire a la certitude que la signature a été produite, ou pas, par un membre du groupe, mais il n'obtient aucune information sur l'identifiant de ce membre, le signataire communique au destinataire uniquement son identifiant chiffré au moyen d'une clé publique de l'autorité de confiance ; la signature est anonyme. Le destinataire a toutefois la possibilité de s'adresser à l'autorité de confiance qui peut déterminer l'identité du signataire à partir de l'identifiant chiffré qui accompagne la signature anonyme de groupe. L'autorité de confiance peut donc lever l'anonymat à tout moment.

Après constitution auprès de l'autorité de confiance, un groupe peut évoluer. Selon un premier type d'évolution, de nouveaux individus peuvent devenir membres du groupe. Selon un deuxième type d'évolution, des membres peuvent disparaître, soit par le départ d'un individu du groupe, soit par l'exclusion d'un individu du groupe ; pour ce type d'évolution, on parle de révocation. A chaque évolution du groupe, l'autorité de confiance est confrontée aux problèmes de donner ou de retirer à un membre du groupe les moyens de produire une signature anonyme du groupe. Le premier problème posé, qui réside dans l'attribution des moyens de produire une signature anonyme du groupe à un nouveau membre, est résolu en utilisant un des algorithmes de génération de clé publique/clé privée connus qui permettent d'associer à une même clé publique autant de clés privées que nécessaire. Un exemple d'un tel algorithme est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997.

Le second problème posé, qui réside dans le fait de retirer à un individu ces moyens, présente différentes solutions connues qui sont des procédés de révocation.

Un premier de ces procédés est décrit dans l'article suivant de E. Bresson et J. Stern, « Efficient Revocation in group Signatures », in K. Kim, editor, Public Key Cryptography – PKC 2001, volume 1992 of LNCS, pages 190-206, Springer-Verlag, 2001. Ce procédé repose sur le fait que chaque membre d'un groupe possède un identifiant qui lui est propre. Etant donné que la signature doit rester anonyme, il n'est pas possible de dévoiler cet identifiant. Toutefois, selon le procédé, l'identifiant du signataire est divisé par celui de chaque membre révoqué ; le résultat de la division est toujours différent de 1 si et seulement si le signataire n'est pas lui-même un membre révoqué. Ensuite, le procédé chiffre, avec un algorithme de chiffrement, chacun des résultats de ces divisions et transmet au destinataire ces résultats chiffrés accompagnés d'éléments déterminés. Le destinataire exploite les éléments déterminés et les résultats chiffrés pour vérifier d'une part que les divisions ont été correctement effectuées et d'autre part que tous les résultats sont différents de 1 ; c'est-à-dire pour s'assurer que la signature a été produite par un membre non révoqué.

Ce procédé a pour inconvénient de générer une signature anonyme de groupe dont la longueur et le temps de calcul augmentent proportionnellement au nombre de membres révoqués étant donné qu'il y a autant de résultats chiffrés et d'éléments déterminés que de membres révoqués.

Un deuxième de ces procédés de révocation est décrit dans l'article de H.J. Kim, J.I. Lim et D.H. Lee qui a pour référence « Efficient and Secure Member Deletion in Group Signature Schemes », In D. Won, editor. Information Security and Cryptology – ICISC 2000, volume 2015 of LNCS, pages 150 et s. Springer-Verlag 2000. Ce procédé consiste à utiliser trois clés supplémentaires en plus des clés nécessaires à la réussite de la signature de groupe : une clé privée de propriété pour chaque membre, une clé publique de propriété pour permettre à chaque membre de vérifier la validité de sa clé et une clé publique de renouvellement permettant à chaque membre de modifier sa clé privée de propriété à chaque fois qu'un membre rejoint ou quitte le groupe. Pour chaque nouveau membre et pour chaque révocation d'un membre, l'autorité de confiance modifie la clé publique de propriété et la clé de renouvellement. Chaque membre restant du groupe modifie sa propre clé privée de propriété à l'aide de la clé de renouvellement et vérifie sa validité grâce à la clé publique de propriété. Lors de la signature électronique d'un message, le membre signataire utilise sa clé privée de propriété. Ainsi, le destinataire peut vérifier la signature électronique à l'aide de la clé publique de propriété. Ce procédé a pour inconvénient d'être d'application particulière car il est prouvé sûre uniquement dans un schéma de signature de groupe particulier qui correspond à celui présenté dans l'article de J. Camenisch, M. Michels, ayant pour référence « A group Signature Scheme with Improved Efficiency », In K. Ohta et D. Pei, editors, Advances in Cryptology – ASIACRYPT'98, volume 1514 of LNCS, pages 160-174. Springler-Verlag, 1998. En outre, ce procédé est désavantageux en ce qu'il impose des calculs à chaque membre à chaque fois qu'un membre rejoint ou quitte le groupe ; or, ces calculs peuvent devenir fréquents si la dynamique du groupe est importante.

Un des objectifs de l'invention est de remédier aux inconvénients des méthodes connues et précédemment décrites.

Exposé de l'invention

A cet effet, l'invention a pour objet un procédé cryptographique de signature anonyme d'un message destiné à être mis en œuvre par un membre d'un groupe, ce groupe étant composé de n membres équipés chacun d'un moyen de calcul et d'un moyen de mémorisation associé. Ce procédé comprend des étapes initiales qui consistent lors de la constitution du groupe :

- dans une première étape, à calculer par un premier moyen de calcul d'une autorité de confiance, une paire de clés asymétriques communes aux membres

du groupe, cette paire de clés se composant d'une clé publique et d'une clé privée communes,

- dans une deuxième étape, à calculer par le premier moyen de calcul une clé publique de groupe associée au groupe,
- dans une troisième étape, pour chaque membre, lors d'une interaction entre le moyen de calcul de l'autorité de confiance et le moyen de calcul du membre, à calculer une clé privée de groupe et à mémoriser cette clé privée de groupe dans le moyen de mémorisation du membre, chaque clé privée de groupe étant associée à la clé publique de groupe et étant différente pour chaque membre du groupe,
- dans une quatrième étape, à déterminer par le premier moyen de calcul autant de clés secrètes symétriques que de membres du groupe,
- dans une cinquième étape, à chiffrer par le premier moyen de calcul la clé privée commune avec chacune des clés secrètes pour obtenir autant de formes chiffrées de la clé privée commune que de membres non révoqués.

Et à chaque révocation au sein du groupe, le procédé comprend des étapes qui consistent :

- dans une sixième étape, à modifier par le premier moyen de calcul la paire de clés asymétriques communes pour déterminer une clé publique et une clé privée communes à jour,
- dans une septième étape, à chiffrer par le premier moyen de calcul la clé privée commune avec chacune des clés secrètes pour obtenir autant de formes chiffrées de la clé privée commune que de membres non révoqués.

Et à chaque signature anonyme d'un message par le membre du groupe, ce message devant être transmis à un destinataire, le procédé comprend des étapes qui consistent :

- dans une huitième étape, à mettre à jour la clé privée commune mémorisée par le moyen de mémorisation du membre uniquement si une des valeurs chiffrées de la clé privée commune est déchiffrable à l'aide de la clé secrète symétrique mémorisée par le moyen de mémorisation du membre,
- dans une neuvième étape, à calculer par le moyen de calcul du membre, une signature dite anonyme du message à l'aide de sa clé privée de groupe,
- dans une dixième étape, à calculer par le moyen de calcul du membre une signature dite additionnelle de l'ensemble composé du message et de la signature anonyme, à l'aide de la clé privée commune du membre.

Le procédé selon l'invention consiste à compléter la signature anonyme d'un message effectuée par un membre avec une signature additionnelle. Cette signature additionnelle est calculée à l'aide d'une copie, détenue par le membre, d'une clé privée de signature identique pour l'ensemble des membres autorisés à signer et inconnue de tous les membres révoqués. Cette clé privée dite commune est mise à jour par l'autorité de confiance à chaque révocation d'un membre du groupe. La mise à jour de la copie détenue par le membre est déclenchée uniquement lors d'une phase de signature anonyme d'un message par ce membre et la mise à jour n'est possible que pour un membre non révoqué.

Ainsi, un membre révoqué est toujours détecté car la signature additionnelle qu'il fournit est nécessairement fausse étant donné qu'il ne possède pas la clé privée commune mise à jour.

Selon un autre objet, un procédé selon l'invention est tel que la constitution du groupe a lieu à une date t1et est tel que les étapes consistent en outre :

- lors de la première étape, à associer par le premier moyen de calcul la clé privée commune à une date de mise à jour égale à t1,
- lors de la troisième étape, à mémoriser par le moyen de mémorisation de chaque membre la date de mise à jour de la clé privée commune,

et est tel qu'à chaque révocation au sein du groupe à une date t2, les étapes consistent en outre :

- lors de la sixième étape, à modifier par le premier moyen de calcul la date de mise à jour pour déterminer une date de mise à jour égale à la date t2,

et est tel qu'à chaque signature anonyme d'un message par le membre du groupe, ce message devant être transmis à un destinataire, les étapes consistent en outre :

- lors de la huitième étape, à mettre à jour la clé privée commune mémorisée par le moyen de mémorisation du membre uniquement si en outre la date de mise à jour mémorisée par le moyen de mémorisation du membre est différente de la date de mise à jour de la clé privée commune mise à jour par le premier moyen de calcul.

Selon un autre objet, un procédé selon l'invention est tel que les étapes consistent en outre :

- lors de la troisième étape, à calculer en outre par le premier moyen de calcul, pour chaque membre du groupe, un identifiant du membre et à mémoriser en outre par le moyen de mémorisation de chaque membre l'identifiant du membre,

et est tel qu'à chaque révocation au sein du groupe les étapes consistent en outre :

- à calculer par le premier moyen de calcul pour chaque nouveau membre du groupe un identifiant.

Selon un autre objet, un procédé selon l'invention est tel que les étapes consistent en outre :

- lors de la troisième étape, à mémoriser par un moyen de mémorisation relié au premier moyen de calcul la clé secrète symétrique de chaque membre, la paire de clés asymétriques communes aux membres du groupe et la clé publique de groupe,

et est tel que pour chaque modification de la composition du groupe qui correspond à une révocation au sein du groupe, le procédé comprend en outre l'étape qui consiste :

- à supprimer la clé secrète du membre révoqué, du moyen de mémorisation relié au premier moyen de calcul,

et est tel que pour mettre à jour la clé privée commune mémorisée par le moyen de mémorisation d'un membre, le procédé comprend en outre les étapes qui consistent :

- à lire par le moyen de calcul du membre, les différentes formes chiffrées de la clé privée commune qui sont mémorisées dans le moyen de mémorisation relié au premier moyen de calcul,
- à déchiffrer par le moyen de calcul du membre et à l'aide de la clé secrète mémorisée par le moyen de mémorisation du membre, les différentes formes chiffrées de la clé privée commune.

L'invention a en outre pour objet un dispositif cryptographique de signature anonyme d'un message numérique qui comprend :

- un premier moyen de calcul pour calculer d'une part au moins une paire de clés asymétriques communes aux membres du groupe composé de n membres et d'autre part une clé publique de groupe associée au groupe, pour calculer pour chaque membre, lors d'une interaction avec le moyen de calcul du membre, une clé privée de groupe, chaque clé privée de groupe étant associée à la clé publique de groupe et étant différente pour chaque membre du groupe, pour déterminer autant de clés secrètes symétriques que de membres du groupe et pour chiffrer la clé privée commune avec chacune des clés secrètes symétriques pour obtenir autant de formes chiffrées de la clé privée commune que de membres non révoqués.

Selon un autre objet, un dispositif selon l'invention comprend en outre :

- un moyen de mémorisation relié au premier moyen de calcul via un réseau de communication pour mémoriser au moins la clé secrète symétrique de chaque membre du groupe, la clé publique de groupe, la clé publique commune aux membres du groupe et chacune des différentes formes chiffrées de la clé privée commune.

L'invention a en outre pour objet une carte à puce destinée à un membre d'un groupe constitué de n membres et destinée à interagir avec un dispositif précédent. Cette carte comprend :

- un moyen de mémorisation d'une clé privée commune aux membres du groupe, d'une clé privée de groupe du membre et d'une clé secrète symétrique attribuée au membre,
- un moyen de mise à jour de la clé privée commune mémorisée par le moyen de mémorisation du membre pour mettre à jour la clé privée commune uniquement si une des valeurs chiffrées de la clé privée commune, calculées par le premier moyen de calcul du dispositif, est déchiffrable à l'aide de la clé secrète symétrique mémorisée par le moyen de mémorisation du membre,
- un moyen de calcul pour calculer une signature anonyme d'un message à l'aide de sa clé privée de groupe et pour calculer une signature additionnelle de l'ensemble composé du message et de la signature anonyme à l'aide de la clé privée commune du membre.

Selon un autre objet, une carte selon l'invention est telle que le moyen de mise à jour comprend un moyen de déchiffrement pour déchiffrer une des valeurs chiffrées de la clé privée commune, calculées par le premier moyen de calcul du dispositif, à l'aide de la clé privée commune mémorisée par le moyen de mémorisation du membre.

Brève description des figures

D'autres caractéristiques et avantages de l'invention apparaîtront lors de la description qui suit et qui est faite en regard de figures annexées de modes particuliers de réalisation donnés à titre d'exemples non limitatifs. Ces figures représentent :

La figure 1 est un organigramme d'un procédé selon l'invention.

La figure 2 est un organigramme d'une réalisation particulière d'un procédé selon l'invention.

La figure 3 est un schéma d'un mode particulier de mise en œuvre d'un procédé selon l'invention.

Description détaillée de modes de réalisation de l'invention

La figure 1 représente un organigramme d'un procédé cryptographique de signature anonyme d'un message selon l'invention. Le procédé est destiné à être mis en œuvre par un membre d'un groupe composé de n membres. Chaque membre possède un moyen de calcul associé à un moyen de mémorisation. Le procédé se déroule en différentes étapes qui comprennent des étapes initiales et des étapes non-initiales. Les étapes initiales interviennent lors de la création du groupe et sont listées ci-après.

Une première étape consiste à calculer 1 par un premier moyen de calcul d'une autorité de confiance, une paire de clés asymétriques communes aux membres du groupe ; cette paire de clés se compose d'une clé publique et d'une clé privée communes. L'algorithme utilisé pour la première étape est un algorithme de signature à clé publique qui peut-être l'algorithme RSA, pour R.L. Rivest, A.Shamir et L. Adleman qui en sont les auteurs.

Une deuxième étape consiste à calculer 2 par le premier moyen de calcul une clé publique de groupe associée au groupe. Le calcul est effectué en faisant appel à un algorithme particulier. Cet algorithme peut être celui décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997.

Une troisième étape consiste à calculer 3 lors d'une interaction entre l'autorité de confiance et chaque membre du groupe pris successivement, une clé privée de groupe associée à la clé publique de groupe, chaque clé privée de groupe étant différente pour chaque membre du groupe. Lors de l'interaction, la clé privée de groupe du membre est mémorisée 4 par le moyen de mémorisation du membre, l'autorité de confiance n'a pas connaissance de cette clé. Le calcul est effectué en faisant appel à un algorithme particulier. Cet algorithme peut être celui décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997.

Une quatrième étape consiste à déterminer 5 par le premier moyen de calcul autant de clés secrètes symétriques que de membres du groupe. Cette détermination peut consister à tirer au hasard des chiffres et des lettres pour former une clé. Selon une variante, les clés secrètes symétriques peuvent vérifier une certaine distribution. Une telle distribution est décrite dans l'article de C.K.Wong, M.G.Gouda et S.S.Lam intitulé "Secure Group Communications Using Key Graph" – Technical Report TR-97-23, 28 juillet 1997.

Une cinquième étape consiste à chiffrer 6 par le premier moyen de calcul la clé privée commune avec chacune des clés secrètes pour obtenir autant de formes chiffrées de la clé privée commune que de membres non révoqués. Le chiffrement est effectué en faisant appel à un algorithme de chiffrement tel que l'algorithme AES.

Selon la variante précédente, les clés secrètes symétriques vérifient une certaine distribution qui permet de ne pas chiffrer la clé privée commune avec chacune des clés secrètes mais avec seulement certaines d'entre elles.

Après constitution, la composition du groupe peut se modifier 7. Une modification consiste soit en une révocation au sein du groupe, soit en l'entrée d'un nouveau membre dans le groupe. A chaque révocation au sein du groupe et optionnellement lors de l'arrivée d'un nouveau membre, le procédé comprend les étapes suivantes.

Une sixième étape consiste à modifier 8 par le premier moyen de calcul la paire de clés asymétriques communes pour déterminer une clé publique et une clé privée communes à jour de la composition du groupe. Cette modification est effectuée en utilisant typiquement le même algorithme que celui utilisé lors de la première étape.

Une septième étape consiste à chiffrer 9 par le premier moyen de calcul la clé privée commune avec chacune des clés secrètes pour obtenir autant de formes chiffrées de la clé privée commune que de membres non révoqués. Ce chiffrement est effectué en utilisant typiquement le même algorithme que celui utilisé lors de la cinquième étape.

A un moment donné quelconque, un membre du groupe peut entreprendre de signer 10 un message avant de le transmettre à un destinataire. A chaque signature anonyme d'un message par le membre, le procédé comprend les étapes suivantes.

Une huitième étape consiste à mettre 11 à jour la clé privée commune mémorisée par le moyen de mémorisation du membre uniquement si une des valeurs chiffrées de la clé privée commune est déchiffrable à l'aide de la clé secrète symétrique mémorisée par le moyen de mémorisation du membre. Le déchiffrement est effectué en utilisant le même algorithme que celui utilisé lors de la septième étape, c'est-à-dire lors du chiffrement. La mise à jour est effectuée si l'algorithme de déchiffrement permet de déchiffrer une des valeurs chiffrées de la clé privée commune.

Une neuvième étape consiste à calculer 12 par le moyen de calcul associé au moyen de mémorisation du membre, une signature dite anonyme du message à l'aide de sa clé privée de groupe. Le calcul est effectué en faisant appel à un algorithme de signature anonyme. Un tel algorithme est décrit dans l'article de J.Camenisch et

M.Stadler qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. Une autre description est donnée dans l'article de J.Camenisch et M.Michels qui a pour référence "A group signature scheme with improved efficiency. In K.Ohta et D.Pei, editors, Advances in cryptology-ASIACRYPT'98, volume 1514 of LNCS, pages 160-174. Springer-Verlag, 1998.

Une dixième étape consiste à calculer 13 par le moyen de calcul du membre une signature dite additionnelle de l'ensemble composé du message et de la signature anonyme, à l'aide de la clé privée commune du membre. L'algorithme utilisé pour la dixième étape est un algorithme de signature à clé publique qui peut-être l'algorithme RSA.

La figure 2 est un organigramme d'une réalisation particulière du procédé selon l'invention. Les éléments déjà décrits en regard de la figure 1 ne sont pas re-décrits. Les éléments particuliers sont décrits ci-après.

La première étape consiste en outre à associer 14 une date de mise à jour égale à t1 à la clé privée commune, en considérant que t1 est la date de constitution du groupe.

La troisième étape consiste en outre à mémoriser 15 par le moyen de mémorisation de chaque membre la date de mise à jour de la clé privée commune.

A chaque modification de la clé privée commune à une date t2 lors de la sixième étape, le procédé consiste en outre à modifier 16 par le premier moyen de calcul la date de mise à jour pour déterminer une date de mise à jour égale à la date t2.

A chaque signature anonyme d'un message par un membre du groupe, ce message devant être transmis à un destinataire, la huitième étape consiste à mettre à jour la clé privée commune mémorisée par le moyen de mémorisation du membre si, en outre, la date de mise à jour mémorisée par le moyen de mémorisation du membre est différente 17 de la date de mise à jour de la clé privée commune mise à jour par le premier moyen de calcul. Par contre, si la date mémorisée par le moyen de mémorisation du membre est égale à la date de mise à jour de la clé privée de groupe mise à jour, il n'y a pas de mise à jour par le moyen de mémorisation du membre.

Tant qu'il n'y a ni révocation, ni entrée d'un nouveau membre, il n'y a pas de mise à jour de la paire de clés asymétriques communes et de la date de mise à jour par le premier moyen de calcul. Par conséquent et de manière avantageuse, le moyen de calcul du membre ne met pas à jour sa clé privée commune, il utilise la clé privée

commune qui est mémorisée dans le moyen de mémorisation du membre pour calculer la signature additionnelle.

La figure 3 est un schéma d'un mode de mise en œuvre d'un procédé selon l'invention au moyen d'un système.

Le système comprend au moins un moyen 20 de calcul et autant de cartes 21_1 à puce que de membres dans le groupe.

Une autorité de confiance, telle une personne physique, une personne morale, une administration nationale ou internationale, détient un moyen 20 de calcul représenté par un serveur sur la figure 3. Ce moyen de calcul 20 est relié par une première liaison 22 de communication à un réseau 23 de communication qui peut aussi bien être un réseau public comme internet, qu'un réseau privé comme un réseau LAN, abréviation des termes anglo-saxons Local Area Network.

Chaque membre d'un groupe détient une carte 21_1 à puce qui comprend dans la puce un moyen 24 de mémorisation et un moyen 25 de calcul. Chaque membre détient en outre, ou a accès à, un lecteur 26 de cette carte relié par une deuxième liaison 27 de communication à un ordinateur 28 personnel, ou tout ordinateur équivalent. L'ordinateur 28 personnel est relié par une troisième liaison 29 de communication au réseau 23 de communication.

La constitution du groupe auprès de l'autorité de confiance se traduit par une interaction entre l'autorité de confiance et chaque membre du groupe. Avant cette interaction, le serveur 20 de l'autorité de confiance calcule une paire de clés 30, 31 asymétriques communes aux membres du groupe et une clé 32 publique de groupe associée au groupe. Lors de chaque interaction, le serveur 20 de l'autorité de confiance et le moyen 25 de calcul du membre calculent une clé 33_1 privée de groupe. La clé 33_1 privée de groupe est mémorisée dans le moyen 24 de mémorisation de la carte à puce du membre. Après interaction avec l'autorité de confiance, le membre possède une clé privée de groupe qui lui est propre et qui est différente de la clé privée de groupe de tous les autres membres. La paire 30, 31 de clés asymétriques communes se compose d'une clé 30 publique commune et d'une clé privée 31 commune. A cette paire 30, 31 peut être associée une date D de mise à jour qui est initialisée à la date t1 de calcul de cette paire. Les clés privées de groupe sont différentes pour chaque membre du groupe et sont associées à la clé 32 publique du groupe.

Lors de chaque interaction, le serveur 20 de l'autorité de confiance détermine une clé 34_1 secrète symétrique. Le serveur 20 chiffre ensuite la clé 31 privée commune

avec chacune des clés 34_i secrètes pour obtenir autant de formes chiffrées de la clé 31 privée commune que de membres non révoqués.

Généralement lors de chaque interaction, le serveur 20 de l'autorité de confiance et le moyen 25 de calcul du membre calculent en outre un identifiant 35_i du membre.

Pendant l'interaction entre l'autorité de confiance et un membre, la carte 21_1 à puce mémorise dans son moyen 24 de mémorisation la clé 31 privée commune, la clé 33_1 privée de groupe du membre et la clé 34_1 secrète attribuée au membre. Le transfert des clés dans une carte à puce est effectué lors de l'interaction par des procédés classiques.

L'autorité de confiance conserve une copie de chacune des clés 34_i secrètes symétriques et identifiants 35_i de chaque membre dans un espace mémoire qui peut être une zone mémoire du serveur 20 ou un moyen 36 de mémorisation associé. Les différentes clés publiques et les valeurs chiffrées de la clé 31 privée commune sont rangées dans un annuaire qui est stocké dans une partie publique de l'espace mémoire 20, 36 ; c'est-à-dire directement accessible, en particulier, par chaque membre du groupe ou, en particulier, par chaque destinataire d'un message et ce par l'intermédiaire du réseau 23.

Après constitution auprès de l'autorité de confiance, le groupe peut évoluer, soit par l'entrée d'un nouveau membre dans le groupe, soit par la révocation d'un membre du groupe.

A chaque révocation au sein du groupe, le serveur 20 modifie la paire de clés 30, 31 asymétriques communes pour déterminer une paire de clés asymétriques à jour de la composition du groupe. Cette mise à jour est effectuée à une date donnée dite de mise à jour. Elle peut aussi être éventuellement effectuée lors de l'entrée d'un nouveau membre dans le groupe.

Après détermination de cette paire de clés asymétriques communes à jour, le serveur 20 met à disposition sous formes chiffrées la clé 31 privée de cette paire de clés asymétriques pour chacune des cartes 21_1 à puce des membres non révoqués du groupe. Le serveur 20 calcule autant de formes chiffrées que de membres non révoqués en utilisant la clé 34_i secrète personnelle à chacun de ces membres. A chaque évolution du groupe, le serveur 20 chiffre la clé 31 privée de la paire de clés 30, 31 asymétriques communes à jour.

A chacune des clés 34_i secrètes personnelles introduite comme argument d'entrée de l'algorithme de chiffrement utilisé correspond un résultat qui est la valeur

chiffrée de la clé 31 privée commune de la paire de clés asymétriques à jour. Les différents résultats et, généralement, la date de mise à jour sont rangés dans l'annuaire.

Lorsqu'un membre du groupe veut signer un message mémorisé dans un ordinateur 28 personnel, il introduit sa carte 21_1 à puce dans le lecteur 26 de carte relié à cet ordinateur 28. Le moyen 25 de calcul de la carte 21_1 à puce se connecte à l'espace 20, 36 mémoire dans lequel est stocké l'annuaire, via l'ordinateur 28 personnel et le réseau 23.

La carte 21_1 à puce lit dans l'annuaire la date D de mise à jour de la clé privée commune. Le moyen 25 de calcul de la carte 21_1 à puce compare cette date D de mise à jour avec celle D_1 qu'elle détient dans son moyen 24 de mémorisation. Soit ces dates sont différentes, soit ces dates sont identiques.

Si les dates sont différentes, la carte 21_1 à puce peut, par exemple, copier dans son moyen 24 de mémorisation les différentes formes chiffrées de la clé 31 privée commune. Le moyen 25 de calcul de la carte 21_1 à puce peut alors entreprendre de déchiffrer chacune des formes chiffrées de la clé 31 privée commune à l'aide de l'algorithme de déchiffrement qui est associé à l'algorithme de chiffrement préalablement utilisé. Les arguments d'entrée comprennent d'une part, la clé 34_1 secrète personnelle mémorisée dans la carte 21_1 à puce et d'autre part, prises successivement, les formes chiffrées de la clé 31 privée commune. Au premier résultat correct de déchiffrement, la carte 21_1 à puce met à jour d'une part la clé 31 privée commune qu'elle détient dans son moyen 24 de mémorisation avec la valeur déchiffrée de la clé 31 privée chiffrée commune et d'autre part la date D_1 de mise à jour qu'elle détient dans son moyen 24 de mémorisation avec la date D de mise à jour associée à la valeur déchiffrée de la clé 31 privée chiffrée commune.

Une autre méthode consiste à placer devant chaque forme chiffrée de la clé 31 privée commune un identifiant du membre concerné. Le moyen 25 de calcul de la carte 21_1 à puce peut alors entreprendre de tester chacune des formes chiffrées de la clé 31 privée commune à l'aide de l'identifiant. Lorsqu'elle arrive à un test valide, elle entreprend alors de déchiffrer la forme chiffrée de la clé 31 privée commune qui lui correspond à l'aide de l'algorithme de déchiffrement qui est associé à l'algorithme de chiffrement préalablement utilisé. Les arguments d'entrée comprennent d'une part, la clé 34_1 secrète personnelle mémorisée dans la carte 21_1 à puce et d'autre part la forme chiffrée de la clé 31 privée commune. La carte 21_1 à puce met à jour d'une part la clé 31 privée commune qu'elle détient dans son moyen 24 de mémorisation avec la valeur déchiffrée de la clé 31 privée chiffrée commune et d'autre part la date D_1 de mise à

jour qu'elle détient dans son moyen 24 de mémorisation avec la date D de mise à jour associée à la valeur déchiffrée de la clé 31 privée chiffrée commune.

Si les dates sont identiques la carte à puce n'effectue pas de copie dans son moyen 24 de mémorisation des différentes formes chiffrées de la clé 31 privée commune. Cette situation se présente lorsque aucune évolution du groupe n'a eu lieu depuis l'entrée du membre dans le groupe ; la carte 21_1 à puce détient la dernière mise à jour de la clé 31 privée commune.

Après cette phase de mise à jour, le moyen 25 de calcul de la carte 21_1 à puce récupère le message mémorisé dans l'ordinateur 28. Le moyen 25 de calcul de la carte 21_1 à puce calcule une signature anonyme de ce message à l'aide de l'algorithme de signature. Les arguments d'entrée comprennent d'une part le message et d'autre part la clé 33_1 privée de groupe mémorisée dans le moyen 24 de mémorisation de la puce.

A l'issue de ce calcul, le moyen 25 de calcul de la carte 21_1 à puce calcule une seconde signature dite additionnelle de l'ensemble formé du message et de la signature anonyme à l'aide de l'algorithme de signature précédent. Les arguments d'entrée comprennent d'une part l'ensemble formé du message et de la signature anonyme et d'autre part la clé 31 privée commune mémorisée dans le moyen de mémorisation du membre.

En final, la carte 21_1 à puce transmet au destinataire choisi par le membre, la signature additionnelle, la signature anonyme et le message.

Le destinataire peut dans ces conditions vérifier que le membre qui a signé le message est un membre non révoqué. A cette fin, le destinataire vérifie chacune des deux signatures, la signature additionnelle et la signature anonyme, à l'aide de la clé publique commune, respectivement de la clé publique de groupe. Pour vérifier, le destinataire utilise un algorithme de vérification disponible par exemple sur un ordinateur 37 personnel. Les arguments d'entrée comprennent d'une part le message et d'autre part la clé publique commune, respectivement la clé publique de groupe.

Une première application d'un procédé selon l'invention est le vote électronique. Le vote électronique se déroule en deux phases :

- une inscription sur une liste électorale auprès d'une autorité administrative,
- une opération de vote auprès d'une urne connectée via un réseau de communication à un serveur d'une administration des votes.

Lors de l'inscription, l'électeur obtient une clé privée de groupe selon un procédé selon l'invention. Dans cette mise en œuvre du procédé, la signature anonyme que pourra produire l'électeur à partir de sa clé privée de groupe est dite "corrélable".

Ceci signifie que, dans le cas où l'électeur tenterait de signer de manière anonyme un second bulletin de vote en produisant une signature anonyme, ce bulletin serait rejeté par l'urne. En effet, la signature anonyme étant corrélable, l'urne est en mesure de vérifier qu'il s'agit d'une seconde signature anonyme.

Un électeur malveillant ne peut pas prétendre avoir perdu sa clé privée de groupe, en recevoir une autre et être en mesure de voter deux fois. En effet, la mise en œuvre d'un procédé selon l'invention permet de lui interdire l'utilisation de la première clé privée de groupe ; cette clé privée de groupe est mise à jour au moment où il déclare avoir perdu la première clé privée de groupe. Cette perte est gérée par la mise en œuvre d'un procédé selon l'invention comme une révocation du membre.

Une seconde application d'un procédé selon l'invention est un service d'enchères électroniques. Les enchères font appel à trois protagonistes : un serveur d'enchères, une autorité de confiance et un client. L'ensemble des clients forme un groupe dit groupe des clients. Un utilisateur désirant s'inscrire au groupe des clients doit s'adresser à l'autorité de confiance qui lui fournit sa clé privée de groupe. Il obtient ainsi le droit de produire une signature anonyme de groupe. Muni de ce droit, il peut signer chacune de ses enchères de manière anonyme. Lors d'une enchère pour un certain produit, chaque membre du groupe des clients peut enchérir en signant un message contenant notamment le produit mis en vente et le montant de son enchère. Le serveur d'enchères peut vérifier l'appartenance au groupe et donc la validité de l'enchère en vérifiant la signature anonyme de groupe. Le vainqueur est celui qui donne la dernière enchère avant l'adjudication. Le dernier message reçu par le serveur d'enchères est donc celui du vainqueur. Le serveur adresse alors ce message et la signature anonyme de groupe correspondante à l'autorité de confiance qui est la seule capable d'en lever l'anonymat et donc de déterminer l'identité physique de l'acheteur du produit mis aux enchères.

Les enchères mettent en jeu des groupes dynamiques : de nouvelles personnes peuvent chaque jour s'inscrire au groupe, un membre peut quitter le groupe ou être exclu pour fraude à tout moment. Il est donc indispensable de mettre en place un système de révocation pour empêcher qu'un membre révoqué ne puisse se servir de sa signature de manière frauduleuse. En effet, le membre révoqué pourrait continuer à utiliser sa clé privée de groupe pour participer aux enchères et fausser le bon déroulement de ces dernières par exemple en faisant monter le montant. Et, s'il prend soin de se retirer suffisamment tôt du processus de façon à ne pas remporter les enchères en question, alors cette fraude n'est pas détectée puisque seule l'identité du

gagnant est finalement révélée. La mise en œuvre d'un procédé selon l'invention permet de résoudre le problème de révocation d'un ou de membre(s) du groupe.

Une troisième application d'un procédé selon l'invention est le paiement électronique. Elle met en jeu quatre protagonistes : un client, un commerçant, une banque et une autorité de confiance. Chaque client doit se faire identifier par le système et obtenir une clé privée de groupe avant de pouvoir effectuer sa première transaction. Pour effectuer un paiement, le client doit retirer des pièces électroniques auprès de sa banque. Les pièces qu'il retire sont anonymes grâce à l'utilisation d'un mécanisme dit de signature aveugle. La dépense d'une pièce C chez un commerçant se fait de la manière suivante : le client génère une signature de groupe portant sur les pièces C et transmet l'ensemble signature et pièces C au commerçant. Le commerçant vérifie la signature de la banque attachée à chaque pièce C et vérifie la signature de groupe. Si chacune des deux signatures est valide, le commerçant accepte la transaction. A un moment donné du jour, le commerçant transmet à sa banque les signatures et les pièces reçues en paiement pour virement à son compte. En cas de fraude, par exemple par la réutilisation d'une même pièce dans plusieurs transactions, la banque envoie la signature de groupe portant sur la pièce litigieuse à l'autorité de confiance afin qu'elle identifie le client indélicat et sanctionne le contrevenant.

Un mécanisme fiable de révocation des clés privées de groupe compromises est nécessaire afin d'éviter une fraude du type suivant : un client malhonnête signale à l'autorité de confiance la perte de sa clé privée de groupe s et décline alors toute responsabilité pour les fraudes qui pourraient être commises avec s. Le client remet sa clé à son complice, lequel peut alors utiliser s pour signer les pièces c qu'il a légitimement retirées à la banque, puis les dépenser autant de fois qu'il le souhaite. Un procédé selon l'invention permet de résoudre le problème de la révocation des clés privées de groupe.

REVENDICATIONS

1. Procédé cryptographique de signature anonyme d'un message destiné à être mis en œuvre par un membre d'un groupe, ce groupe étant composé de n membres équipés chacun d'un moyen (25) de calcul et d'un moyen (24) de mémorisation associé, caractérisé en ce qu'il comprend des étapes initiales qui consistent lors de la constitution du groupe :
   - dans une première étape, à calculer (1) par un premier moyen de calcul d'une autorité de confiance, une paire de clés (30,31) asymétriques communes aux membres du groupe, cette paire de clés se composant d'une clé (30) publique et d'une clé (31) privée communes,
   - dans une deuxième étape, à calculer (2) par le premier moyen de calcul une clé (32) publique de groupe associée au groupe,
   - dans une troisième étape, pour chaque membre, lors d'une interaction entre le moyen de calcul de l'autorité de confiance et le moyen de calcul du membre, à calculer (3) une clé (33_1) privée de groupe et à mémoriser (4) cette clé (33_1) privée de groupe dans le moyen (24) de mémorisation du membre, chaque clé (33_1) privée de groupe étant associée à la clé (32) publique de groupe et étant différente pour chaque membre du groupe,
   - dans une quatrième étape, à déterminer (5) par le premier moyen de calcul autant de clés (34_i) secrètes symétriques que de membres du groupe,
   - dans une cinquième étape, à chiffrer (6) par le premier moyen (20) de calcul la clé (31) privée commune avec chacune des clés (34_i) secrètes pour obtenir autant de formes chiffrées de la clé (31) privée commune que de membres non révoqués,

   et en ce qu'à chaque révocation au sein du groupe, le procédé comprend des étapes qui consistent :
   - dans une sixième étape, à modifier (8) par le premier moyen (20) de calcul la paire de clés (30, 31) asymétriques communes pour déterminer une clé (30) publique et une clé (31) privée communes à jour,
   - dans une septième étape, à chiffrer (9) par le premier moyen (20) de calcul la clé (31) privée commune avec chacune des clés (34_i) secrètes pour obtenir autant de formes chiffrées de la clé (31) privée commune que de membres non révoqués,

et en ce qu'à chaque signature (10) anonyme d'un message par le membre du groupe, ce message devant être transmis à un destinataire, le procédé comprend des étapes qui consistent :

- dans une huitième étape, à mettre (11) à jour la clé (31) privée commune mémorisée par le moyen (24) de mémorisation du membre uniquement si une des valeurs chiffrées de la clé (31) privée commune est déchiffrable à l'aide de la clé (34_1) secrète symétrique mémorisée par le moyen (24) de mémorisation du membre,
- dans une neuvième étape, à calculer (12) par le moyen (25) de calcul du membre, une signature dite anonyme du message à l'aide de sa clé (33_1) privée de groupe,
- dans une dixième étape, à calculer (13) par le moyen (24) de calcul du membre une signature dite additionnelle de l'ensemble composé du message et de la signature anonyme, à l'aide de la clé (31) privée commune du membre.

2. Procédé cryptographique de signature anonyme selon la revendication 1, dans lequel la constitution du groupe a lieu à une date t1 et dans lequel les étapes consistent en outre :
   - lors de la première étape, à associer (14) par le premier moyen de calcul la clé (31) privée commune à une date de mise à jour égale à t1,
   - lors de la troisième étape, à mémoriser (15) par le moyen (24) de mémorisation de chaque membre la date de mise à jour de la clé (31) privée commune,

   et dans lequel à chaque révocation au sein du groupe à une date t2, les étapes consistent en outre :
   - lors de la sixième étape, à modifier (16) par le premier moyen (20) de calcul la date de mise à jour pour déterminer une date de mise à jour égale à la date t2,

   et dans lequel à chaque signature anonyme d'un message par le membre du groupe, ce message devant être transmis à un destinataire, les étapes consistent en outre :
   - lors de la huitième étape, à mettre (11) à jour la clé privée commune mémorisée par le moyen (24) de mémorisation du membre uniquement si en outre la date (D_1) de mise à jour mémorisée par le moyen (24) de mémorisation du membre est différente de la date (D) de mise à jour de la clé (31) privée commune mise à jour par le premier moyen de calcul.

3. Procédé cryptographique de signature anonyme selon la revendication 1, dans lequel les étapes consistent en outre :
   - lors de la troisième étape, à calculer (3) en outre par le premier moyen de calcul, pour chaque membre du groupe, un identifiant (35_i) du membre et à mémoriser (4) en outre par le moyen (24) de mémorisation de chaque membre l'identifiant (35_i) du membre,

   et en ce qu'à chaque révocation au sein du groupe les étapes consistent en outre :
   - à calculer par le premier moyen (20) de calcul pour chaque nouveau membre du groupe un identifiant (35_i).

4. Procédé cryptographique de signature anonyme d'un message selon la revendication 3, dans lequel les étapes initiales consistent en outre :
   - lors de la troisième étape, à mémoriser par un moyen (36) de mémorisation relié au premier moyen (20) de calcul la clé (34_i) secrète symétrique de chaque membre, la clé (32) publique de groupe, la clé (30) publique commune aux membres du groupe, chacune des différentes formes chiffrées de la clé (31) privée commune et chacun des identifiants (35_i), chaque forme chiffrée de la clé (31) privée commune étant associée à un des identifiants (35_i),

   et dans lequel pour chaque modification de la composition du groupe qui correspond à une révocation d'un des membres du groupe, le procédé comprend en outre l'étape qui consiste :
   - à supprimer la clé (34_i)secrète de ce membre, du moyen (36) de mémorisation relié au premier moyen (20) de calcul,

   et en ce que pour mettre à jour la clé (31) privée commune mémorisée par le moyen (24) de mémorisation du membre le procédé comprend en outre les étapes qui consistent :
   - à lire par le moyen (25) de calcul du membre, la forme chiffrée de la clé (31) privée commune qui est mémorisée dans le moyen (36) de mémorisation relié au premier moyen (20) de calcul et associée à l'identifiant (35_i) du membre,
   - à déchiffrer par le moyen (25) de calcul du membre et à l'aide de la clé (34_i) secrète mémorisée par le moyen (24) de mémorisation du membre, la forme chiffrée de la clé (31) privée commune précédemment lue.

5. Procédé cryptographique de signature anonyme d'un message selon la revendication 1, dans lequel les étapes initiales consistent en outre :
   - lors de la troisième étape, à mémoriser par un moyen (36) de mémorisation relié au premier moyen (20) de calcul la clé secrète de chaque membre, la paire de clés (30, 31) asymétriques communes aux membres du groupe et la clé (32) publique de groupe,

   et dans lequel pour chaque modification de la composition du groupe qui correspond à une révocation au sein du groupe, le procédé comprend en outre l'étape qui consiste :
   - à supprimer la clé secrète du membre révoqué, du moyen (36) de mémorisation relié au premier moyen (20) de calcul,

   et en ce que pour mettre à jour la clé (31) privée commune mémorisée par le moyen (24) de mémorisation d'un membre le procédé comprend en outre les étapes qui consistent :
   - à lire par le moyen (25) de calcul du membre, les différentes formes chiffrées de la clé (31) privée commune qui sont mémorisées dans le moyen (36) de mémorisation relié au premier moyen (20) de calcul,
   - à déchiffrer par le moyen (25) de calcul du membre et à l'aide de la clé (34_1) secrète mémorisée par le moyen (24) de mémorisation du membre, les différentes formes chiffrées de la clé (31) privée commune.

6. Dispositif cryptographique de signature anonyme d'un message numérique, caractérisé en ce qu'il comprend :
   - un premier moyen (20) de calcul pour calculer (1, 2) d'une part au moins une paire de clés (30, 31) asymétriques communes aux membres du groupe composé de n membres et d'autre part une clé (32) publique de groupe associée au groupe, pour calculer (3) pour chaque membre, lors d'une interaction avec le moyen (25) de calcul du membre, une clé (33_1) privée de groupe, chaque clé (33_1) privée de groupe étant associée à la clé (32) publique de groupe et étant différente pour chaque membre du groupe, pour déterminer (5) autant de clés (34_i) secrètes symétriques que de membres du groupe et pour chiffrer (6) la clé (31) privée commune avec chacune des clés (34_i) secrètes symétriques pour obtenir autant de formes chiffrées de la clé (31) privée commune que de membres non révoqués.

7. Dispositif cryptographique de signature anonyme d'un message numérique selon la revendication 6, dans le dispositif comprend en outre :
   - un moyen (36) de mémorisation relié au premier moyen (20) de calcul via un réseau (23) de communication pour mémoriser au moins la clé (34_i) secrète symétrique de chaque membre du groupe, la clé (32) publique de groupe, la clé (30) publique commune aux membres du groupe et chacune des différentes formes chiffrées de la clé (31) privée commune.

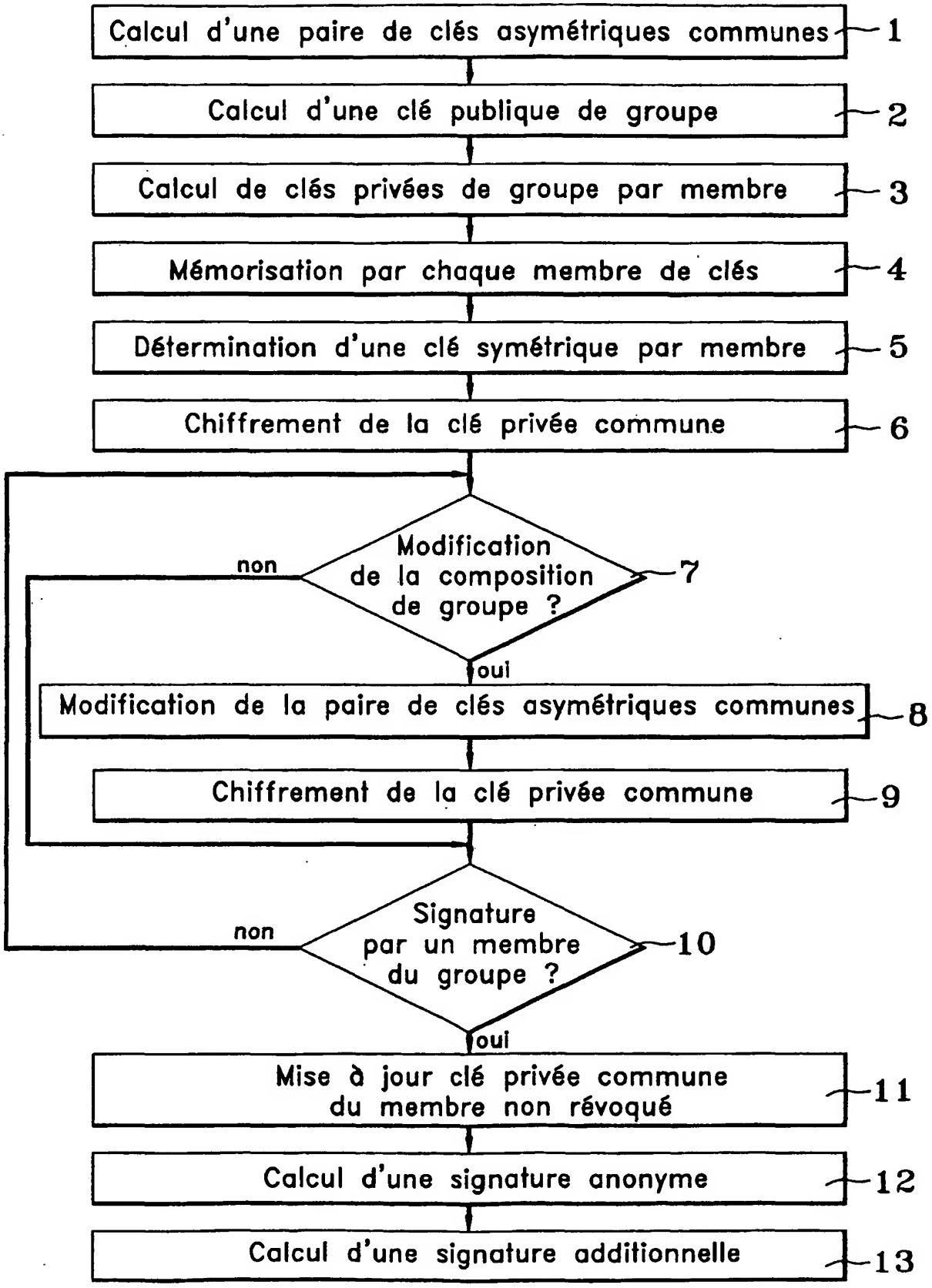
8. Carte (21_l) à puce destinée à un membre d'un groupe constitué de n membres et destinée à interagir avec un dispositif selon l'une des revendications 6 et 7, caractérisé en ce qu'elle comprend :
   - un moyen (24) de mémorisation d'une clé (31) privée commune aux membres du groupe, d'une clé (33_l) privée de groupe du membre et d'une clé (34_l) secrète symétrique attribuée au membre,
   - un moyen (25) de mise à jour de la clé (31) privée commune mémorisée par le moyen (24) de mémorisation du membre pour mettre (11) à jour la clé (31) privée commune uniquement si une des valeurs chiffrées de la clé (31) privée commune, calculée par le premier moyen (20) de calcul du dispositif, est déchiffrable à l'aide de la clé (34_l) secrète symétrique mémorisée par le moyen (24) de mémorisation du membre,
   - un moyen (25) de calcul pour calculer (12) une signature anonyme d'un message à l'aide de sa clé (33_l) privée de groupe et pour calculer (13) une signature additionnelle de l'ensemble composé du message et de la signature anonyme à l'aide de la clé (31) privée commune du membre.

9. Carte (21_l) à puce selon la revendication 8 dans laquelle le moyen (25) de mise à jour comprend un moyen de déchiffrement pour déchiffrer une des valeurs chiffrées de la clé (31) privée commune, calculée (1) par le premier moyen (20) de calcul du dispositif, à l'aide de la clé (34_l) secrète symétrique mémorisée par le moyen (24) de mémorisation du membre.

10. Système cryptographique de signature anonyme d'un message numérique destiné à mettre en œuvre un procédé selon la revendication 1, caractérisé en ce qu'il comprend :
   - au moins un dispositif selon l'une des revendications 6 et 7 et

- au moins autant de cartes (21_1) à puce selon la revendication 8 que de membres dans le groupe.

FIG. 1


Calcul d'une paire de clés asymétriques communes
1
Calcul d'une clé publique de groupe
2
Calcul de clés privées de groupe par membre
3
Mémorisation par chaque membre de clés
4
Détermination d'une clé symétrique par membre
5
Chiffrement de la clé privée commune
6
Modification de la composition de groupe ?
7
non
oui
Modification de la paire de clés asymétriques communes
8
Chiffrement de la clé privée commune
9
Signature par un membre du groupe ?
10
non
oui
Mise à jour clé privée commune du membre non révoqué
11
Calcul d'une signature anonyme
12
Calcul d'une signature additionnelle
13

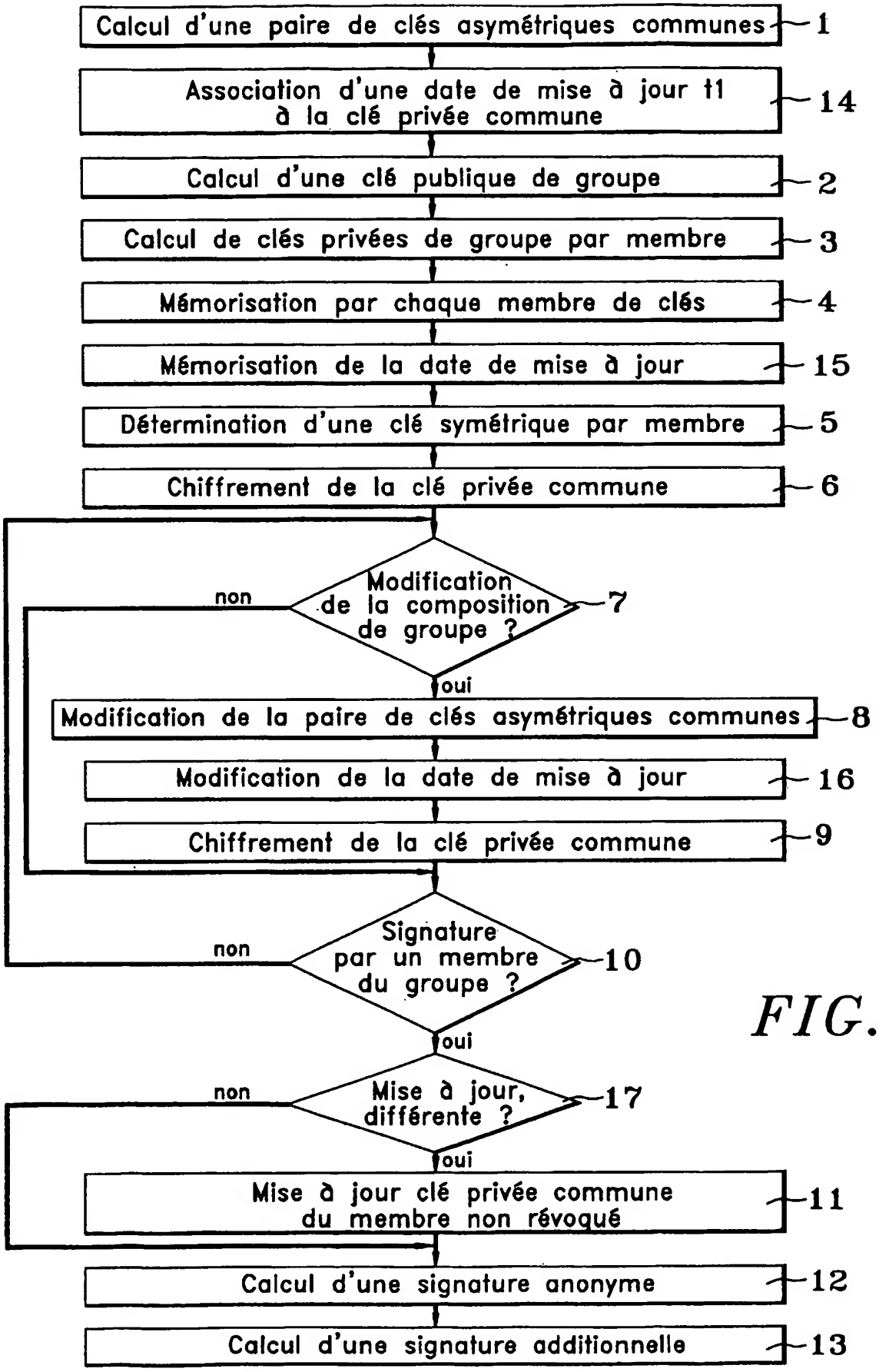
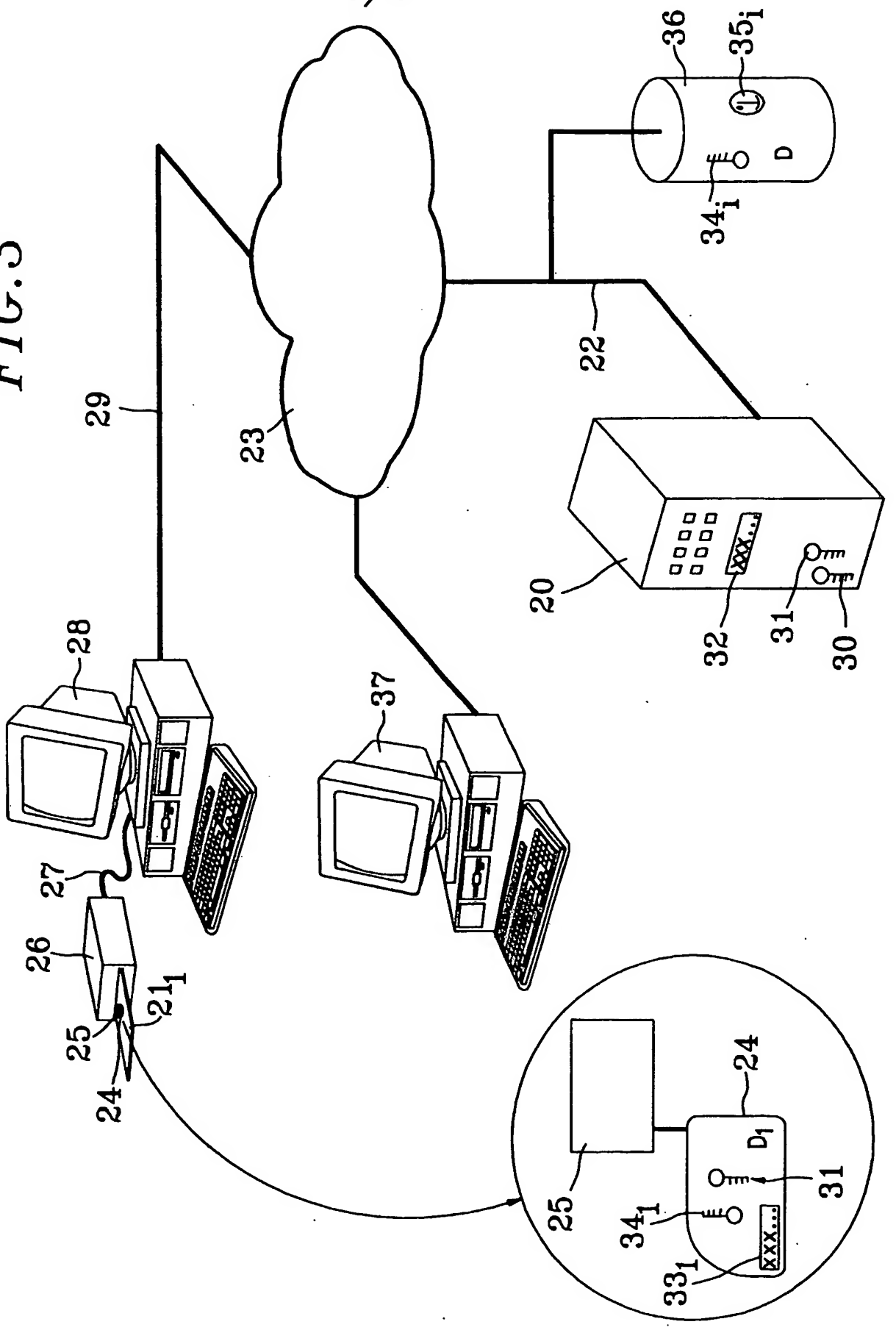

Calcul d'une paire de clés asymétriques communes
1
Association d'une date de mise à jour t1 à la clé privée commune
14
Calcul d'une clé publique de groupe
2
Calcul de clés privées de groupe par membre
3
Mémorisation par chaque membre de clés
4
Mémorisation de la date de mise à jour
15
Détermination d'une clé symétrique par membre
5
Chiffrement de la clé privée commune
6
Modification de la composition de groupe ?
7
non
oui
Modification de la paire de clés asymétriques communes
8
Modification de la date de mise à jour
16
Chiffrement de la clé privée commune
9
Signature par un membre du groupe ?
10
non
oui
Mise à jour, différente ?
17
non
oui
Mise à jour clé privée commune du membre non révoqué
11
Calcul d'une signature anonyme
12
Calcul d'une signature additionnelle
13

FIG.2

FIG.3



INTERNATIONAL SEARCH REPORT

Int[redacted]pplication No
PCT/F[redacted]2/04335

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	H.J. KIM, J.I. LIM, D.H. LEE: "ICISC 2000 - LNCS 2015 - p. 150-161: Efficient and Secure Member Deletion in Group Signature Schemes" 2001 , SPRINGER-VERLAG , BERLIN XP002218345 cited in the application abstract page 152, line 41 -page 153, line 15 page 155, line 8 -page 159, line 9 --- -/--	1,6

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 May 2003	26/05/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In nal Application No
PCT/F 02/04335

C.(Continuation) DOCUMENTS CONSIDERED BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	E. BRESSON, J. STERN: "Public Key Cryptography PKC 20001 - p. 190-206: Efficient Revocation in Group Signatures" 2001 , SPRINGER-VERLAG , BERLIN XP002218346 cited in the application abstract page 198, line 1 -page 201, line 17	1,6

RAPPORT DE RECHERCHE INTERNATIONALE

Der Internationale No
PCT/[redacted]02/04335

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	H.J. KIM, J.I. LIM, D.H. LEE: "ICISC 2000 - LNCS 2015 - p. 150-161: Efficient and Secure Member Deletion in Group Signature Schemes" 2001 , SPRINGER-VERLAG , BERLIN XP002218345 cité dans la demande abrégé page 152, ligne 41 -page 153, ligne 15 page 155, ligne 8 -page 159, ligne 9 --- -/--	1,6

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 mai 2003	26/05/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/[redacted]02/04335

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	E. BRESSON, J. STERN: "Public Key Cryptography PKC 20001 - p. 190-206: Efficient Revocation in Group Signatures" 2001 , SPRINGER-VERLAG , BERLIN XP002218346 cité dans la demande abrégé page 198, ligne 1 -page 201, ligne 17	1,6